Khoa Công nghệ Thông tin
fit@hcmus

NHẬP MÔN MÃ HOÁ MẬT MÃ

THỰC HÀNH TUẦN 4

Tên: Bạch Minh Khôi

MSSV: 19127181

Lớp: 19MMT

I. Cách biên dịch và chạy mã nguồn:

Chạy trực tiếp bằng file RSA.py hoặc có thể dùng Visual Studio Code, PyCharm,…

Có thể test từng tính năng bằng cách comment từng block code ở dưới __main__.

II. Thuật toán:

- **Ý tưởng chính:** Dựa theo mã ASCII của từng chữ cái để mã hoá và giải mã theo thuật toán mã hoá RSA.
- **Chi tiết thuật toán:**

1. Tạo public key và private key:

- Hàm **keyGen(numSize)** nhận vào numSize để generate ra cặp số nguyên tố p và q có độ dài numSize.
- Tính **n=pq, phi=(p-1)(q-1)**.
- Chọn e bằng hàm **calcE(phi)** dựa vào giá trị của phi bằng cách:
  For e in range(3, phi, 2):
  If **isPrime(e)**:
  If **isCoPrime(phi, e)**:
  Return e
  Giải thích: ngoài 2 thì các số nguyên tố đều là số lẻ, tìm e bằng cách thử từng số lẻ bắt đầu từ 3. Nếu e là số nguyên tố và e là số nguyên tố cùng nhau với phi thì trả về e.
  Lý do không xét coPrime(n, e): làm tăng tốc độ xử lí vì đối với n và phi rất lớn thì sự khác biệt giữa n và phi là không đáng kể, có thể xem các số nguyên tố cùng nhau với phi sẽ là số nguyên tố cùng nhau với n.
- Tính giá trị của d bằng cách:
  Chọn d bằng thuật toán Euclid mở rộng, nếu d tìm được là số âm thì d += phi cho tới khi d là số dương.
- Viết cặp khoá tìm được vào file **“rsa_pub.txt”, “rsa.txt”** và trả về cặp khoá publicKey = (e, n) và privateKey = (d, n).

2. Mã hoá message bằng encrypt(publicKey, message).

- Dùng mảng cipher=[] để lưu trữ tạm các giá trị dùng để tạo cipherText.
- Mã hoá từng kí tự của message bằng cách chuyển nó sang giá trị ASCII và mã hoá theo thuật toán RSA theo công thức **c=(m^e)%n** và thêm giá trị tìm được vào mảng cipher.

- Trả về chuỗi cipherText bằng cách dựa vào độ dài của số n và thêm padding là các kí tự “0” vào trước từng phần tử của mảng cipher để mỗi phần tử đều có độ dài giống n.
  Viết chuỗi cipherText vừa tìm được vào file **“encrypted.txt”.**

3. Giải mã cipherText bằng decrypt(privateKey, message).

- Dùng hàm **collectCipherArray(cipher, n)** để thu thập mảng các số đã được mã hoá bằng cách dựa vào độ dài của số n và chuyển mỗi n-kí tự trong chuỗi cipherText thành số và đưa vào mảng kết quả sau đó trả về kết quả lọc được.
- Dùng mảng plain = [] để lưu trữ các giá trị giải mã được từ mảng cipherArray theo công thức **m = (c^e)%n**.
- Ghép từng giá trị trong mảng plain thành chuỗi, ghi kết quả vào file **“decrypted.txt”** và trả về plainText cần tìm.